Logging you, Logging me: A Replicable Study of Privacy and Sharing Behaviour in Groups of Visual Lifeloggers

Journal Item

Logging you, Logging me: A Replicable Study of Privacy and Sharing Behaviour in Groups of Visual Lifeloggers

BLAINE A. PRICE, Computing and Communications, The Open University
AVELIE STUART, Psychology, University of Exeter
GUL CALIKLI, Computer Science and Engineering, Chalmers and University of Gothenburg
CIARAN MCCORMICK, Computing and Communications, The Open University
VIKRAM MEHTA, Computing and Communications, The Open University
LUKE HUTTON, Computing and Communications, The Open University
AROSHA K. BANDARA, Computing and Communications, The Open University
MARK LEVINE, Psychology, University of Exeter
BASHAR NUSEIBEH, Computing and Communications, The Open University & Lero, University of Limerick

Low cost digital cameras in smartphones and wearable devices make it easy for people to automatically capture and share images as a visual lifelog. Having been inspired by a US campus based study that explored *individual* privacy behaviours of visual lifeloggers, we conducted a similar study on a UK campus, however we also focussed on the privacy behaviours of *groups* of lifeloggers. We argue for the importance of replicability and therefore we built a publicly available toolkit, which includes camera design, study guidelines and source code. Our results show some similar sharing behaviour to the US based study: people tried to preserve the privacy of strangers, but we found fewer bystander reactions despite using a more obvious camera. In contrast, we did not find a reluctance to share images of screens but we did find that images of vices were shared less. Regarding privacy behaviours in *groups* of lifeloggers, we found that people were more willing to share images of people they were interacting with than of strangers, that lifelogging in groups could change what defines a private space, and that lifelogging groups establish different rules to manage privacy for those inside and outside the group.

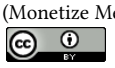
CCS Concepts: • **Human-centered computing → Empirical studies in ubiquitous and mobile computing**; • **Security and privacy → Social aspects of security and privacy**; **Usability in security and privacy**;

General Terms: Ubiquitous Computing, Privacy

Additional Key Words and Phrases: Visual Lifelogging, Privacy, Replication, wearable cameras

ACM Reference format:
Blaine A. Price, Avelie Stuart, Gul Calikli, Ciaran McCormick, Vikram Mehta, Luke Hutton, Arosha K. Bandara, Mark Levine, and Bashar Nuseibeh. 2017. Logging you, Logging me: A Replicable Study of Privacy and Sharing Behaviour in Groups of Visual Lifeloggers. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 1, 2, Article 22 (June 2017), 18 pages.
DOI: http://dx.doi.org/10.1145/3090087

The authors acknowledge partial support from EPSRC grants EP/K033433/1, EP/K033522/1 (Privacy Dynamics), EPSRC grant EP/L021285/1 (Monetize Me) as well as the ERC Advanced Grant - Adaptive Security and Privacy (291652 - ASAP), and SFI grant 3/RC/2094.



 2474-9567/2017/6-ART22 $15.00
DOI: http://dx.doi.org/10.1145/3090087

1 INTRODUCTION

Automatic visual lifelogging was once the domain of ubiquitous computing pioneers, such as Steve Mann [28] or the original Microsoft SenseCam developers [17]. Today consumer level devices such as the GoPro (https://gopro.com/) for recording individual sports and recreation, the Narrative Clip (NC2, unavailable due to restructure at time of writing) [31] and Snapchat Spectacles [39], make visual lifelogging possible for anyone. Automatic wearable cameras aside, the fact that most people carry a manually operated camera at all times in the form of their smartphone has made the constant sharing of images an everyday activity. Any image taken in a public place carries a privacy risk, but it is the images taken automatically by lifelogging cameras that carry the greatest risk, as they are not under direct user control. We were inspired by the work of Hoyle at al. [20] who explored the individual privacy behaviours of visual lifeloggers among undergraduates in a US university campus setting. With the growing ubiquity of individuals with non-wearable cameras constantly taking and posting images on social media, we were also interested in how privacy behaviours would change when groups of people were all wearing cameras. In the next sub-section we discuss the relevant privacy theory and research questions we sought to address.

1.1 The Privacy Behaviours of Multiple Visual Lifeloggers

Visual lifelogging, in particular the sharing of the captured images, needs to be carefully managed by users in order to protect their own and other people's privacy [18]. The main differences between conventional and lifelogging cameras is that lifelogging cameras capture a larger volume of images, and that image capture is passive and automatic, i.e. the timing and composition of each image capture is not chosen by the camera wearer [22]. Although bystanders that the wearer is interacting with may be aware that they are being photographed (if the lifelogger informs them about the camera) they do not know the precise moment that they are being captured. This means that while general consent might be given by a bystander to be photographed, the wearer still has to make post-hoc judgments about the bystander's privacy when reviewing the images. There will also be bystanders who are unaware of the camera, and have thus not given explicit consent.

These types of privacy management practices have interpersonal elements, because they require communication with bystanders or, where communication is not possible, for the wearer to infer the bystanders' preferences. These inferences could be based on the individual's own preferences, or based on social norms [3]. Moreover, bystanders may fear sanction if they resist privacy invasions and this can result in lack of obvious resistance on their part [29], meaning that lifeloggers may be required to interpret others' secret preferences. People may thus feel an obligation to protect the privacy of others even when others do not ask them to (see [5, 35]). We have anecdotal reports in our early work that bystanders were reluctant to ask lifeloggers about their cameras, in particular they often assumed it was a medical device.

Not all decisions to turn off the camera or delete photographs will be based on privacy, however. Impression management behaviour [14] - how lifeloggers manage the attention that wearing a camera brings, and how they respond to people's looks or comments (e.g., Google Glass was criticized for its appearance, as well as the privacy concerns it raised [12]) - might inter-relate with privacy behaviours, or be mistaken for privacy behaviours because they manifest in the same way. For example, choosing not to wear a camera in a particular setting could be due to feeling inappropriately attired and not wanting to draw attention to oneself, rather than the belief that the bystanders in that setting do not wish to be photographed for privacy reasons. To try and provoke behaviour and conversation around this issue, we added an occasionally flashing LED to our camera to explore whether the LED enabled bystanders further opportunity to enquire about the camera, and how this feature made the lifeloggers become more aware of both their privacy and their appearance.

In the Hoyle et al. [20] study we use as a basis for our study, they gave 36 undergraduates a lifelogging camera (composed of an Android phone running custom software) to wear around their neck. They provided features to

pause recording, delete recent images, as well as to review images afterwards and delete them or indicate which they would be comfortable sharing within a certain category of people. The frequency of these decisions was used as a proxy for privacy behaviour. In addition to the considerations examined by Hoyle et al, it seems apparent that studies of visual lifelogging should consider more than just the individual lifelogger. We suggest that the popularity of visual lifelogging is likely to increase; therefore we are interested in how lifeloggers interact with each other and treat each other's privacy. Previous privacy theory and empirical research has found that privacy regulation can be shared amongst members of a group [2, 35] - but this has never been studied in the context of visual lifelogging, as far as we know. New research questions arise in the context of co-lifelogging and privacy. For instance - is there a difference in privacy behaviours when interacting with or capturing other lifeloggers, compared to bystanders? Does being a lifelogger imply consent, such that lifeloggers feel less need to protect other lifeloggers' privacy? These questions inspired us to ask groups of people to wear lifelogging cameras.

We were also interested in expanding Hoyle et al.'s analysis of how setting might influence privacy decisions. To do this we code images based on location categories - with the expectation that there might be locations participants treat as more or less private, as well as coding the category of bystanders within the images (i.e., whether someone is a lifelogger, non-lifelogger friend, or stranger), whether the lifelogger and bystanders appear to be interacting with each other, and the type of objects within the images (e.g., alcohol, computer screens). Each of these is aimed to add context to the images that might explain whether people keep, delete, or share images.

1.2 Building the Cameras and Replicability

Initially our study was intended to be a replication study, but the first problem we faced was finding appropriate camera hardware that would allow the major features of Hoyle et al.'s study [20] to be replicated. The Microsoft Sensecam and its commercial spin off are no longer available and other commercial off-the-shelf (COTS) cameras, such as the (then available) NC2 wearable camera, were not suitable for this study for 3 reasons. Firstly, to access the images taken by the camera required a proprietary application to be installed on the participant's computer. We felt this would result in a higher level of non-compliance. Secondly, the NC2 had an upper limit on the photo interval of 120 seconds which would create too many images for participants to review (in [20] the interval was 300 seconds). Finally, the NC2 was relatively expensive when compared to the cost of building a device ourselves (note: by the time we wrote this paper the company had recently gone bankrupt). Hoyle et al. used a custom modified Android firmware, which is no longer available, and current Android releases do not allow apps to access the camera without being explicitly activated by the user. The newest releases of Android require root access to the device to allow the camera to take images without any user interaction. Rooting a device that could contain images of a personal nature exposed participants to an undue security risk that we felt would be an unethical research practice.

Upon finding we could not easily replicate the previous study and in light of recent concerns in the psychology literature about an inability to replicate many results from publications in top journals [34], we sought to understand the state of replicability in pervasive and ubiquitous computing in order to make our study replicable. Many experiments use proprietary and undocumented hardware, such as Vasilescu et al.'s development of autonomous underwater vehicles [41], or complex environments which are difficult to replicate in the wild, such as city-scale sensor networks [38]. Wilson et al. argues that replication yields rewards, such as improving the reputation of the community, improving confidence in findings, and enhancing teaching [45]. Increased awareness of the value of replicability is filtering through to the HCI literature, with more researchers sharing their data, methods, and scripts for analyses [30]. In this paper, we adapt and extend a study which was not inherently replicable into one which is itself replicable, with source code, methodological details and hardware designs made openly available. We chose a long established widely used open hardware platform for our camera system [25]. Although this will eventually become deprecated, our open design will allow researchers to update the system with changes in the technology landscape.

1.3 Research Questions

Our initial research questions mirror those of [20]:

RQ1: How do lifeloggers manage collection of images and in particular the deletion of unwanted images, or prevent the logging of images?
RQ2: What characteristics of the images and the environment make the lifelogger more or less likely to share an image?
RQ3: How do lifeloggers report the reactions of bystanders?

To adapt these questions to specifically address our study, on how behaviour changed when an entire social group wore lifelogging cameras as opposed to individuals, our extended research questions are as follows.

In terms of how the lifelogger behaves:

RQ2.1: Does the presence of other lifeloggers in images make the lifelogger more or less likely to share images?
RQ2.2: If a person captured in an image is unknown to the lifelogger, does this make the lifelogger more or less likely to share the image?

In terms of how bystanders behave:

RQ3.1: How do bystanders react to more obvious indicators of the camera (e.g. flashing LEDs and signs)?
RQ3.2: Do bystanders who are known to the lifelogger react differently from strangers?

And in terms of being around other lifeloggers:

RQ4: How do people report behaving and feeling about wearing a lifelogging camera when they are around other lifeloggers, compared to non-lifeloggers?

Answers to these questions will provide insights into the privacy issues in a near future when more people will be wearing lifelogging cameras. Moreover, we explain our study in sufficient detail and make camera hardware design, source code, questionnaires and interview questions publicly available to enable replication of this research study.

2 RELATED WORK

The RepliCHI movement has identified challenges to replicability which resonate with the ubicomp community. Lallemand et al. find that as concepts and terminology in HCI are fast-changing, it can be difficult to meaningfully replicate a study after a long period of time, where the same concept may invite two wildly different interpretations over time [26]. For example, between the time of Hoyle et al.'s study and ours, fast-changing cultural norms about self-photography such as the emerging "selfie era" [40], could manifest in significantly different results. Similarly, Patil notes that replicating privacy studies is difficult as people's privacy attitudes and competencies evolve along with technology, making it difficult to attribute a cause to differences in results [44]. In our study, we had to design hardware to approximate the conditions of Hoyle et al.'s study, however Carlson et al. note that trying to maintain consistent parameters in hardware replications can be difficult, particularly where the differences are difficult to quantify [8].

Privacy is a notoriously difficult concept to define, and has been operationalized in several ways in the literature. While Westin argues that privacy is a form of control over information [43], Gavison defines privacy as limited access to the self, in terms of the extent to which one is known, physically accessible, or the subject of attention [13]. Nissenbaum's contextual integrity [32] posits that privacy is maintained by context-specific norms, which consider when it is appropriate for information to be transmitted, and to whom, rather than information itself being inherently public or private. These contrasting perspectives have implications for how we frame the privacy concerns of bystanders. For example, considering privacy in terms of control mechanisms does not account for the experiences of bystanders who are unable to extend any control over how their information is used, nor adopt defensive behaviours when they are unaware they are being surveilled. Conversely, by considering the

privacy expectations of bystanders in public situations, contextual integrity can provide a means of diagnosing the appropriateness of such technologies.

Gurrin et al. [15] note a number of novel privacy challenges in visual lifelogging, including:

(1) the increasing resolution of captured images and inclusion of other metadata such as locations,
(2) the lack of curation meaning potentially sensitive contexts are captured making the systematic redaction of individuals or locations difficult,
(3) the lack of consent from bystanders,
(4) the permanence of captured images,
(5) the ability to construct false narratives from a subset of collected data which could have legal implications, and
(6) the security of the captured data.

Hoyle et al. [20] provide a concise summary of the literature on visual lifelogging and some of the related privacy issues, however most of this work assumes that individual lifeloggers are the only ones with cameras. More recently, Clinch et al. [11] reported a study involving an instrumented house with fixed cameras where 13 participants also had wearable cameras. They intentionally chose a remote location to exclude the possibility of accidentally capturing bystanders. Despite the closed environment with multiple lifeloggers, over time periods less than 10 minutes they had a relatively low percentage of reciprocal images, that is, one lifelogger capturing another whose camera captured the first. They also found that lifeloggers frequently forgot to switch off their camera when entering private places and those that did often forgot to switch back on when exiting. A major concern for their participants, however, was the capture of possibly confidential information on open laptop screens and phones. This was also noted in Hoyle et al.'s more recent analysis [19] and Korayem et al. [24] propose a framework to automatically address this issue. While Chowdhury et al. [10] find that lifeloggers exhibit little concern for the privacy of bystanders, other work [9] from the perspective of bystanders finds many are unwilling to have their images used without consent, with privacy preferences depending on the context and content of the photos. The authors argue lifelogging applications must understand context in order to make appropriate privacy decisions.

One aspect of constant still and video recording is that it becomes normalized and no longer noticed. Portnoff et al. [36] saw this effect with webcam indicator lights on laptops. One of Koelle et al.'s [23] recommendations was that devices that can record images should have some kind of indicator to show when this is happening, yet current small COTS lifelogging cameras (e.g. [31] [39]) are designed to be unobtrusive and not draw attention, hence they are not suitable for our interest in looking at the effect of drawing attention to the camera.

3 METHODOLOGY

In this section, we give details of our camera design as well as provide information about the source code for the software running the camera and the image reviewing software used by participants. We also describe the protocol for participants and the post-study image coding method we used. All these materials, including flyers for participant recruitment, consent forms, instructions for participants, questionnaires given to participants and image coding protocol together with image coding analyses results are available in our public repository at https://github.com/vllstudy16/vllstudy16.

3.1 Camera Design

We built a wearable and programmable camera with various off the shelf components packed together in a 3D printed red plastic box of size 65x65x22 mm (see Fig. 1, components and build instructions are explained in CameraBuild-Report.pdf in the repository). The wearable camera runs on a 2000 mAh rechargeable LiPo battery. It can effectively work for an entire day and then needs to be charged overnight through the micro USB slot

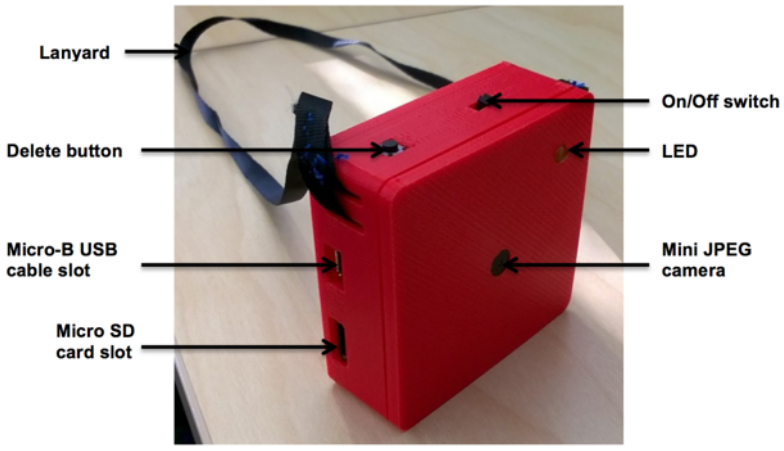


Fig. 1. Lifelogging camera given to participants.

provided. Our design differed from [20] in that we did not include GPS logging (because of power requirements) but we did include an LED to draw attention to the camera. In order to keep the camera design simple we did not include a pause button, instead relying on people to switch off or hide the camera as the button added complexity and we had no easy way to indicate that the camera was recording again.

A user can wear the camera around their neck and move around. The LED flashes once when the wearable camera is switched on (it remains on if there is an error, like a missing SD card). It takes automatic pictures of 640 × 480 pixel resolution and stores them in the micro SD card. The software running on the Arduino microcontroller creates different directories for each day, each storing pictures taken on that particular day. Images are stored with the naming convention: < *hour_minutes_seconds* > and are taken 5 minutes apart. Some more features of the life-logging camera are:

(1) Push button on top: deletes any images taken in the last 5 minutes and logs a timestamp in a text file.
(2) "Random LED flash" mode: Activated by switching on camera with button pressed. The LED then blinks with 2 consecutive flashes with 0.5 second duration with a gap of at least 15 minutes (so that it is not predictable to bystanders and thus they will be more likely to notice it). The start and end flash time is logged in a text file, also stored on the SD card.

3.2 Image Reviewing Software

The image reviewing application was developed using Java 8, which required participants to have this Java version installed on their personal computers. Java was chosen as it is cross-platform (could be used on GNU/Linux, OS X and Windows XP through to Windows 8) and development had a low barrier to entry. Java 8 was chosen over Java 7 since it has better support for Java FX, which made developing a GUI that could be correctly displayed on any resolution screen much easier. The participants were asked to remove the micro-SD card from the camera each evening and insert it into their laptop using the micro-SD to USB converter device provided. They were then instructed to launch the image reviewing application (see subsection 3.7 - Daily Image Review).

3.3 Pilot Testing

The cameras and image reviewing software were piloted on two Psychology PhD candidates, which allowed us to improve the instructions and questionnaires. Participants also requested adjustable neck straps to fit the camera over their heads and allow the camera to sit in a comfortable position.

3.4 Recruitment and Enrollment

Groups of undergraduate students on a large university campus (University of Exeter, UK) were recruited through an online paid participant pool run by the Psychology department. Participants were all at least 18 years old, and all were in pre-existing friendship groups or shared accommodation. Participants were given information and consent forms to read and sign. They were told that none of their raw data would be published, and that they were free to withdraw at any time. Participants answered a questionnaire, and received their cameras and instructions for use. They were asked to wear the camera from that point onwards, unless they were in a context where it was uncomfortable to do so, or it was not permitted. Participants returned to the lab approximately 5 days later (e.g., Monday-Friday), where they answered a final questionnaire and participated in an interview. The camera given to each participant (see Fig. 1) had a label on it saying "University of Exeter - Photography in progress", with the "LED flash" mode activated.

3.5 Ethical Considerations

The study was approved by University of Exeter's IEB, who had particular concerns about people sharing images on social media without express permission. Following [20], and the concerns of our IEB we developed the following list of "Do's and Don'ts" to give participants:

- Respect rules about taking images in public places (e.g., if you see a "no photography allowed" sign).
- Respect other people's wishes to not be photographed. If anyone objects to you wearing the camera in their presence, then put it in your pocket. If anyone asks that a photo of them be deleted simply press the delete button. When you review the images if you see an image of someone who requested that you not photograph them please delete it at that time.
- Please delete images with any nudity. It is specifically prohibited to keep (or share) images of naked people or images that would otherwise compromise an individual's safety or reputation.
- If you observe other members participating in this study using the technology inappropriately or illegally, please get in contact with the researcher.

As with [20] we emphasized to participants that they must respect the privacy of bystanders and gave them "business cards" that contained the researchers contact details, so they could hand them to bystanders to request further information. No bystanders made contact with the researchers.

3.6 Daily Image Review

The participants were asked to review their images at the end of each day using the software we supplied, which automatically logged their answers to a JSON file. The step-by-step procedure for reviewing images was:

- Participants were instructed to delete images that should be immediately deleted (e.g., containing nudity, locations where photography was prohibited, or of people who had asked not to be photographed);
- They were asked to tick reasons for deleting images;
- They were asked to mark images that were blurry or contained no usable information;
- The software presented them with all of the times that day that they used the delete button, including an image prior to deletion (to prompt their memory), and asked why they used the delete button at that time;

- Next, participants were shown all images they had not deleted, and, following [20], were asked if they would not be comfortable sharing them with 3 classes of groups - "Close friends and family," "Other friends and family," "Co-workers, classmates, and acquaintances,", or if they would share it with "Everyone"; and
- Finally, participants answered questions about why they would or would not share these images; for images they said they would not share they were asked how embarrassed or angry they would be if the images were shared.

3.7 Questionnaires and Interview

Participants completed questionnaires at the beginning and end of the study. The questionnaires were adapted from [20], and we added further measures of privacy attitudes [5][43][42] and added questions for how long they have known each other, and how they know each other. The end of study questionnaire repeated the privacy measures and included questions about how they felt while wearing the camera. The interview questions were designed in line with our research questions - including how they felt wearing the camera, the specific behaviours they engaged in to manage the camera, and the reported reactions of bystanders. The full content of these materials are available on our public repository at https://github.com/vllstudy16/vllstudy16.

3.8 Compensation

Participants were given GBP 7 per day up to 5 days (Max: GBP 35 ≈ USD 50), depending on the number of days they completed. Participants were also put into a prize draw for an iPad mini.

3.9 Image Content Analysis

Following Hoyle et al. [20] we developed an initial coding scheme and four people from the research team coded ten random images. This team met to discuss the coding and make some adjustments to clarify unspecified criteria that emerged during the initial coding. The final coding scheme was then carried out on all of the remaining images. One person coded each photograph, and then approximately 30% of all images were randomly selected and coded by a second coder. Inter-rater reliability was calculated on all categorical fields, using Krippendorf's alpha[16], and all codes included in the analysis reached substantial or excellent agreement (from $\alpha = .75 - .85$). The coding instructions and final results from our coders may also be found in the repository.

4 FINDINGS

The findings are organized as follows: we first report on the participant demographics and general privacy attitudes (4.1), and then we outline participant in-situ collection and deletion practices (4.2). The next subsection (4.3) is an analysis of sharing decisions made in the daily image review, based on the presence of subjects, objects, and locations in the images, followed by a subsection (4.4) on the participants reflections in the interviews on their camera use, deletion and sharing practices, and finally a subsection on the effects of the design features of the cameras (4.5). Although we do conduct multiple tests, we have maintained the alpha to determine significance at .05 because we argue that finding an effect where one does exist (i.e. avoiding Type II error) is more important at this stage, than reducing false positives (i.e. Type I error) [4], and point to the sharing percentages as containing more meaningful information about the importance of each finding. We also note that all findings require future replication.

4.1 Participants

Seven groups of between 2-6 participants (26 in total) were run over 5 day periods from January to March, 2016. One participant withdrew from the study after the camera did not work the first day. There were 16 women and 10 men. The majority identified themselves as British (19) and were in their first year of university (24). Nearly

Table 1. Total images captured, kept, shared

	Number
Total images captured	5,628
Total deleted images	1,656 (29%)
Range and average kept per participant	15-308, 103.6
Corrupt or unusable images	1,390 (25%)
Uses of delete button (by number of participants)	77 (14)
Most uses of delete button by one participant	21
Total kept images shared with everyone	2,031 (79%)
Total images not comfortable sharing with close family/friends and/or other family/friends and/or acquaintances	452 (17%)
Total images not comfortable sharing with anyone	49 (.019%)
Images unaccounted for	50 (.02%)

half were studying Psychology (11), and within each group they were all house/flatmates or enrolled in the same degree program (having known each other for an average of 8.3 months).

All reported regular use of Facebook, the majority (19) reported use of Instagram, and Snapchat (16), and half use Twitter (13). Most said they were comfortable being tagged in images online ($M = 6.23$, 9-pt scale), with a reported monthly average frequency of sharing images online ($M = 5, SD = 1.96$, 9-pt scale). We used an adapted Westin privacy measure [7] taken before participants started using the cameras ($\alpha = .68, M = 5.2, SD = .99$, on a 9-pt scale where a higher score reflects higher privacy concern). These privacy attitudes were not correlated with any sharing or deleting behaviour [33]. We categorized the distribution of the sample into Privacy Fundamentalists, Privacy Pragmatists, and Privacy Unconcerned categories [21], however most participants were Pragmatists and too few participants were in the Fundamentalist and Unconcerned categories to make any comparison.

We also measured other-contingent privacy [5] (i.e. assessing whether people believe their privacy depends on the behaviour of others) with 4-items on a 9-pt scale ($M = 4.77, SD = 1.59, \alpha = .85$); and 5-items measuring respect for others privacy ($Median = 7.6, SD = 1.2, \alpha = .90$) [5]. Respect for others' privacy had a ceiling effect, and was not correlated to any sharing or deleting behaviour, however those scoring high on other-contingent privacy were less likely to want to share images with anyone ($r = -.550, p = .012$) (taking into account the total number of images captured per participant).

4.2 In-situ Image Collection and Deletion Practices

Participants said that they tended to do most of their deletion through the end of day review rather than using the in-situ delete button. However, some reported turning the camera off when they were doing the same activity for an extended period, to avoid having to delete images later (although one said it was because they were embarrassed that they didn't do much that day). Table 1 presents the overall numbers of images kept, deleted, and shared. Details of particular note are that that the participant who used the delete button 21 times stated it was for 'no reason' or 'other reason', and that the images unaccounted for would have been caused by participants deleting them directly from the SD rather than through the app. Corrupt or unusable images refer to images that participants marked as blurry, dark, or corrupt.

Although 14 participants used the delete button, some mentioned accidentally pressing it. Only 4 people said that they purposely used it, which was a much lower rate than found by [20]. Most said there was never an occasion that they realized that did not want captured (except one participant when she had just taken cash out) and that they preferred to delete the images at the end of the day, through the software. In contrast with

Table 2. Images shared by location and content

Feature	Number shared	% shared	Feature	Number shared	% shared	Significant Difference?
Indoors	2191	80.3	Outdoors	267	83.5	No
Other people present	1076	78.7	No other people present	1399	81.9	Yes
Other lifeloggers present	89	80.2	Other people present	847	78.7	No
Computer monitor visible	387	80.4	Computer monitor not visible	282	80.9	No
Alcohol and vices present	116	62.1	No alcohol or vices present	2359	81.4	Yes

other studies [11], only one of them reported forgetting to take the camera off for the bathroom or other private spaces. These management techniques are consistent with the findings of [20] on RQ1 although our design did not include a pause button so we could not measure how often they switched off or hid the camera other than as reported in interviews.

4.3 Daily Review Sharing Decisions: Image Subjects, Objects and Location

This section draws on data from the image reviewing software and the image coding. As seen in Table 2, fewer images were shared when other people are in them, than pictures with no people in them ($\chi^2 = 4.0, df = 1, p = 0.046$). This suggests that the presence of other people makes lifeloggers less likely to share images, and is in general consistent with Hoyle et al. [20]. However privacy decisions are likely made based on the lifeloggers' relationship with the bystander or the social context, so to investigate this at a finer level we categorized the human subjects (collectively referred to as 'bystanders') in the captured images into strangers, group members, and non-participant friends, as well as categorising locations. In the following sub-sections we look at how these data address our research questions.

4.3.1 Presence of Bystanders in Images. RQ2.1 asked whether participants treat images of other lifeloggers any differently to images of other people, and our results indicate that they do not. Slightly more images were shared when another participant is in them, to when other non-participants are present, but this difference was not significant ($\chi^2 = 0.13, df = 1, p = 0.72$).

In order to address RQ2.2, we compared sharing results for images with people who were interacting with the participant with sharing results for images where people were not interacting with the participant (coded based on their proximity and orientation to the camera, "known" versus "unknown"). Our results show that lifeloggers are less likely to share images of "unknown" people compared to images of "known" people (72.5% vs. 81.7%,$\chi^2 = 11.5, df = 1, p < 0.001$), To account for whether these decisions are influenced by whether people are recognizable in the images, we also found that even when faces are visible (i.e. not obscured or hidden from the camera), lifeloggers are less likely to share images of "unknown" people than images of "known" people (68.4% vs. 79.5%, $\chi^2 = 5.1, df = 1, p = 0.024$) .

4.3.2 Location. Participants wore the cameras in a range of locations including lecture halls, the gym, shops, pubs, trains, and church. The places participants reported turning off or removing cameras were the bank, public toilets, and in workplaces that are restricted to the public or customer facing.

The location appeared to have a small effect on sharing behaviour with outdoor locations slightly more likely to be shared than indoor (see Table 2, $\chi^2 = 1.6, df = 1, p = 0.212$), although this was not significant. We did a more fine-grained analysis by categorizing locations as "bathroom", "bedroom", "dorm room", "living area/flat or kitchen", "indoor public" and "outdoor public". According to our findings, people were less likely to share images taken in "bathroom" compared to the rest of the locations (35% vs 80.5% on average for the rest of the location categories, $\chi^2 = 1.6, df = 1, p < 0.001$). This suggests that, in answer to RQ2, for our participants among locations only "bathroom" reduced sharing behaviour.

4.3.3 Presence of Screens and Vices (alcohol/tobacco). While [20] found a significant difference in sharing when a screen was present, we found no significant effect with near identical sharing percentages ($\chi^2 = 0.001, df = 1, p = 0.975$). Separating images based on screens with visible content as opposed to others (screen closed or blurred content or no screen) revealed a similar result (80.4% vs. 80.5%, $\chi^2 = 0.008, df = 1, p = 0.929$). From the image reviewing software we can see that only 15 images had screens visible where they chose not to share even with close friends. The ticked reasons for not sharing these images included 4 information privacy reasons, and 10 other-privacy related reasons (It would be embarrassing to share it, It would have violated someone else's privacy, Objects (other than people) in the photo, Participant was in the photo, People within the photo) and 12 non-privacy related reasons (e.g. uninteresting content). In the interviews one participant shed light on this question, saying that it was just "normal stuff or Netflix or my Facebook, that doesn't really matter". Thus, from what we can observe, participants in this study appeared mostly unconcerned about sharing visible screens.

The qualitative results from [19] suggest that lifeloggers choose not to share images with vices such as alcohol or cigarettes and our quantitative findings support this. Images containing alcohol are less likely to be shared than those without (see Table 2, $\chi^2 = 26.4, df = 1, p < 0.001$) and sharing behaviour does not change even when faces are visible (62.3% vs. 80.0%, $\chi^2 = 7.9, df = 1, p < 0.001$) or when the person is known to the lifelogger (60% vs. 78.6%, $\chi^2 = 13.3, df = 1, p = 0.005$). This addresses RQ2 in that vices decrease likelihood of sharing and indicate a stronger privacy threat regardless of whether or not the subject in the image is a stranger.

4.4 Interviews: Interactions with Bystanders and Reflections on Sharing Decisions

This section draws on the interview data to address RQ3 - on the behaviour of bystanders, and RQ4 - how lifeloggers behave around other lifeloggers and non-lifeloggers. This section has been organized around the themes that emerged from the interview transcripts.

4.4.1 Lifelogging at Home with and without Other Lifeloggers. The home is typically understood as the ultimate example of a private domain, however for those who shared a house with other lifeloggers, their reported level of privacy concern while wearing the cameras at home varied depending on whether there were also non-lifeloggers living in the same residence. Two of the groups who lived together said it was very easy being around each other at home, and that they just did their usual activities, such as watching TV together ("At home it's okay for us because we know the place, so it was very familiar.").

Living at home with other non-lifeloggers was usually more problematic. All groups reported asking for express permission from their non-participating flat/housemates, with the exception of one group who said they did not think to ask their other flatmate (this person was apparently "surprised but found it funny"). One participant who had non-lifelogger flatmates reported feeling fine using the camera in her bedroom, but when she went into the kitchen she felt she was being intrusive ("it's our little safe space and I wander around in my pajamas with my hair up and not okay to face the world and so do they. I felt like at times I could really be encroaching on that with having a camera."), although she also said her flatmates did not appear concerned. However, another participant heard through another flatmate that one person in her house "felt weird about it [the camera]", but never said anything to her directly. This statement provides evidence that sometimes bystanders may not feel able to deny access despite feeling discomfort.

Despite this, no one reported difficulty in respecting their housemates' wishes. One participant who was asked by a flatmate not to take images reported becoming very quickly used to turning the camera on and off every time they were in the same room ("I wasn't aware that I was wearing it until I saw someone that didn't want to be photographed because then I was like, 'Oh yes, I had that conversation with them,' and then I'd remember I was wearing it"). Thus they reported a high degree of ease in transitioning between private and public spaces, or managing requests for privacy from people that they lived with.

4.4.2 Lifelogging around Non-participant Friends. Four participants said that their housemates, friends, or boy/girl-friends were initially wary but soon relaxed, e.g.: "Two of the boys at first were a bit like, 'Oh, I'm going to avoid you, I don't want to be on camera.' I was like, 'I can delete any images you don't want,' and they were like, 'Oh actually it's quite funny,' and just ended up posing in front of it instead."

This initial wariness could emerge for a number of reasons - one reason identified by a participant was that her friends were initially worried about being captured, but once they learnt that she had control over the images and could delete them, they then consented to being in the images. This demonstrates that a level of interpersonal trust in others to protect our privacy can be reassuring and relates to the definition of 'privacy as control'.

One participant reported not wearing the camera to her first meeting with her boyfriend's childhood friend ("they're a big part of his life so I didn't want to be just like this weird girl with a camera"). This concern would appear to be related to impression management rather than privacy, a point we come back to again later in the section on Comfort with Lifelogging.

4.4.3 Lifelogging around Strangers. In general, consistent with [20], participants reported few bystanders having problems with being photographed. In terms of questions from strangers, one participant reported that when he went to the pub strangers leaned in to read the sign on his camera, but did not say anything. Another said that the only stranger who asked about the camera was a cashier. Only one participant reported ignoring a stranger's question about the camera (they said they kept walking down the street). The higher interest level (although few objections) from friends compared to the relative lack of interest from strangers suggests that in answer to RQ3.2 we see a greater effect from known as opposed to unknown bystanders. There are a number of reasons why this might be the case, which we discuss later in Section 6.

Images containing strangers in the backgrounds were generally reported by participants as not private - for example, one person said they did not worry because "sometimes, like, for example, in the gym or in the library, there were 1000 people. It was a lot of faces.", implying that these faces could not be distinguished. Another theme around this question was the idea that if people did not know they were being captured then it won't affect them ("chances are that would be in the background of a selfie anyway"), although one participant did say that he felt there was some problems with recording people trying to go about their everyday lives, but this was in reference to the prospect of visual lifelogging become more popular in the future. These findings suggest that the reason why fewer photos of "unknown" people were shared than "known" may be because participants were less interested in sharing them rather than greater concern for strangers' privacy.

4.4.4 Reflections on Decisions to Keep or Delete Images of Bystanders. Unlike Hoyle et al. [20], only seven participants reported being asked to delete images (and only by one or two individuals each). The people asking were non-participant flatmates or friends, never strangers. This relative lack of concern from friends and apparent absence of concern from strangers suggest that in answer to RQ3 bystanders are overall largely unconcerned, however we elaborate some of the variations to this below.

Despite the apparent lack of concern from others, all participants said that they thought about the privacy of others. Yet their management of the images differed somewhat from [20]. All participants said they deleted images of people who requested it, but of those who reported noticing people being uncomfortable but who did not explicitly ask for their images to be deleted, 3 participants said they did delete the images anyway, while 2

others said they did not. An example of the reason given for not deleting images was, "because I thought it's only going to the researcher, but it wouldn't be the kind of picture that I'd do much with. I wouldn't say, 'Oh, let's put this on some massive social media platform and share it with the world."' Another person said their deletion of pictures of others depended on what the other people were doing - "A lot of them, they were either just eating or sitting down, and so I felt that there was nothing too bizarre about them, or things that they wouldn't like other people to see, so I didn't delete any of them." This reflects the research showing that people make judgments about others' privacy preferences[5].

Thus to address RQ1, the understanding that the images would never be shared beyond the researchers influenced their decisions (e.g., "because we know that it won't be published online or anything, or publically, so it doesn't matter if there's embarrassing images because no one will recognize us anyway."). Others said that the fairly mundane content of the images meant that they didn't mind the images being shared.

4.4.5 Reflections on Treatment of Images of Other Lifeloggers vs Non-participant Friends. In the interviews, participants conveyed their decisions about whether to keep or delete images based on whether they were with other lifeloggers or non-lifeloggers. We were interested in understanding whether being a lifelogger implies consent (RQ2.1). There was some variation between the groups in response to this question. One group of lifeloggers said that they discussed what they would do with each other's images and agreed they would not post them on Facebook but they did share images of each other on their (pre-existing) WhatsApp group, "I didn't hesitate to put up the funny images of you [speaking to other participant] on to the group chat, whereas ... whereas I didn't put the funny one of my flatmate up on the flat chat." Therefore, they presumed it was acceptable to keep images of the other lifeloggers, but not to post them anywhere else without permission.

Another group said that for them the same standards applied to other lifeloggers and non-lifelogger friends (also reflected in the quantitative results on sharing), "So if it was like with a group of friends, like some with and some without cameras, if I got a really horrendous picture of them I'm like, 'They're not going to like that. I will delete that.' It was the same principle if I got one of you guys [other lifeloggers] and you weren't looking your best, I would just delete it." These findings suggest that their pre-existing friendship norms guided their lifelogging behaviour.

4.5 The Effects of Specific Design Features of the Cameras

4.5.1 Comfort with Lifelogging. Further discussions in the interviews revealed that sometimes participants' concern about the camera was more about their appearance than privacy ("It was when I walked outside I was like that's a bright red thing there that people are going to notice that."). Thus wearing the camera at home was sometimes reported to be more comfortable than wearing it in public for this reason, rather than concern about the privacy of others or themselves. One group also said they felt less conspicuous when the group of them was wearing the cameras together, despite this drawing more stares from bystanders.

Further interview responses showed a range of feelings about their comfort wearing the camera. A couple of participants reported discomfort with seeing images of their lives - such as food they were eating, or games they were playing on their phone. Despite this the same people said that at times they forgot they were wearing a camera, one even fell asleep with it on. Therefore, it could be that people feel comfortable wearing the camera, but may not be comfortable with the images captured during that time when reviewing them later; or vice versa.

In the end of study questionnaires participants were asked to rate how comfortable they were (on a scale of 1=not at all, 9=very comfortable). "How comfortable were you around others using a life logging camera?" was high (Median=7, SD=1.67), as was "how comfortable were you in using the life logging camera during this study while in private (e.g. at home)?" (Median=8, SD=1.13). "How comfortable were you in using the life logging camera during this study while in public?" was also above the midpoint, but lower than the other comfort measures and had greater variability (Median=6, SD=2.17). This supports some of the qualitative findings explained above.

As a further indicator of their interest in lifelogging, we asked if they are interested in purchasing a camera in the future - the mean was low overall (M=3.04, SD=1.9, 9 pt-scale), but had a bi-modal distribution, indicating some were interested but others were not at all.

4.5.2 Effects of the Camera's More Obvious Features. The LED flash on the camera was intended to invite further queries from bystanders (RQ3.1). While participants reported that bystanders sometimes questioned the flash (and if it meant that it was taking a photograph), none reported it triggering discomfort from bystanders. However, a couple of female participants did report that their friends wanted to clarify that they were not staring at their chests, but that the camera's flashing LED had caught their attention. Therefore, it did create some social difficulty, but not in relation to the image capture per se. Three participants speculated that the camera had intentionally been made big and red to draw attention, but said they would have preferred it was more unobtrusive.

Unexpectedly, images where the LED flashed were slightly more likely to be shared with everyone (55.52%) than images with no flash (51.17%, $\chi^2 = 4.24, df = 1, p = 0.04$). One possible explanation is that if bystanders notice the camera flashing, then in the image they would be looking directly at the camera, making it a more interesting image and thus worth sharing; conversely, covert images where the bystander is unaware they are being captured are less likely to be shared. However this difference is not large and is only one factor involved in sharing decisions.

In an exceptional case, one participant's sign was not on her camera, and reported that people thought she was wearing a heart monitor. This agrees with our previous anecdotal observations of lifelogging cameras in the UK where bystanders assumed a lifelogging camera was a medical or disability assistance device and therefore did not ask questions about it. This may also go some way towards explaining the lack of comment from strangers in this study.

Despite these attempts to make sure bystanders inquired about the camera, there were so few reports that, in answer to RQ3.1, we find that the features added to draw attention to the camera had almost no effect except to make participants more uncomfortable (although this could have an indirect effect on their privacy behaviour, such as choosing not to wear the camera in some locations).

5 THREATS TO VALIDITY AND LIMITATIONS

We measured a relatively small population of undergraduates for a week which will not generalize to other populations or long term use. We also did not measure actual image sharing, we only asked participants who they would hypothetically share with and actual behaviour may differ. The knowledge that images will not be shared beyond the researchers is a genuine threat to the validity of the results, but is not one that we can ethically foresee overcoming, except perhaps by recruiting actual lifeloggers (who would differ from a student sample in numerous ways).

The volume of images captured would also likely affect the way that people treat them, as a matter of cognitive load rather than privacy. Future studies could try asking participants to review fewer pictures, or over a shorter time period, however this would not be typical of lifelogging practice.

The default wording of the questions on the daily image review - who they would not feel comfortable sharing with - assumes that people can imagine their audiences correctly [1], and there may be different results if participants were asked who they would feel comfortable sharing with.

Drawing from the interviews, we see suggestions that there may be other specific location sensitivities that we did not capture in the coding, or that may require specialist knowledge. For example, one participant reported being uncomfortable wearing the camera on the underground (subway train) when they went to London. Another group said they wore the cameras to the student bar, but not a public one, because they felt that other students

would be more understanding. This we could not distinguish in the coding, without verifiable location information. Use of GPS data would help here.

6 DISCUSSION

This paper presents an open source toolkit comprising the source code, hardware designs, questionnaires and study guidelines needed to inexpensively replicate a study investigating privacy behaviours among groups of visual lifeloggers. While much research in this area is difficult to replicate due to the use of proprietary or obsolete hardware and software, this toolkit demonstrates how replicability in this domain can be upheld. Using the toolkit, we conducted a field study to identify which privacy management behaviours manifest in a UK campus setting with groups of lifeloggers.

In common with previous work [20] we found that lifeloggers are willing to share most images and most participants use the post-hoc image review to manage images rather than in-situ. In summary, what did seem to exert an effect on sharing decisions was: bathroom (location), known vs unknown bystanders, the presence of alcohol/cigarettes, and the camera flash.

The novel contributions of this paper include a finer level of analysis of bystander and location categories. For location, that we did not find location differences (except for bathrooms) for sharing decisions is probably because in private locations with other people present they are not likely to keep the camera on. Our qualitative results showed emerging changes in social norms when groups of lifeloggers lived together. That the home could become more private than an open space, due to everyone present wearing a lifelogging camera, is an interesting example of the blurring of public and private contexts caused by technology [6].

As with [20] we found indications of people actively protecting the privacy of bystanders but unlike [20] we had statistically significant evidence for this. Moreover, we found that if a person captured in the image is a stranger to the lifelogger, this makes the lifelogger less likely to share the image (RQ2.2). We also provided evidence that this was not related to the recognisability of the image subject. We did not find a quantitative difference in image sharing behaviour when images contained other lifeloggers as opposed to non-lifeloggers (RQ2.1), but anecdotally some of the participants seemed to deem images of other lifeloggers as less private overall, but referred to their pre-existing social group norms to guide their behaviour.

On the subject of bystander reaction (RQ3) we found fewer reactions than [20] even though our camera had more features to draw attention to it (RQ3.1). This raises several suggestions to be explored in further research - it may be a growing lack of concern for lifelogging in the general public, or that strangers did not know what the device was, or that they did not feel comfortable inquiring about the camera. However, we did find friends of lifeloggers reacted much more than strangers and each lifelogger created social rules around lifelogging among friends and fellow lifeloggers (RQ4). It is interesting that despite greater reports of reactions from known than unknown bystanders, participants were more likely to share pictures of known bystanders. This means that motivations to protect the privacy of people they know can be overridden by motivations to share with their friends [46]. Further investigation into this topic could be undertaken by adding questions to the daily photo review process about their relationships to the image subjects. Moreover, there may be a normalization or adjustment period, whereby some people may be initially ambivalent about being photographed, but after seeing the cameras for a while they consented. This would affect behaviour over time, and thus a time-sensitive analysis might shed insight into changes in privacy behaviour over that adjustment period. It also became clear from our study that the image content and the experience of capturing the image are not always going to have the same privacy implications. In particular we note that discomfort with lifelogging is multi-faceted, e.g. one group said they were more comfortable lifelogging in a group despite everyone looking at them, indicating that people can be more comfortable breaking social norms as a group. This would also reflect the non-normative nature of lifelogging for this sample of UK students, whose experiences might differ from people involved in quantified-self communities [11].

We found some different results from Hoyle et al., in particular, participants in our study were not concerned about sharing images of screens. There could be a number of reasons for this, including the types of activities they are doing on the computer, or because our sample was mostly psychology students, whereas Hoyle et al. had a majority of computer science students, who would be more technology and privacy aware.

6.1 Takeaway Messages and Suggestions for Future Work

Our overall observations support the findings of [27] showing that context for privacy is multi-faceted and governed by individual perceptions, but also that participants inferred in-group contextual norms around both privacy and self-presentation concerns [37]. More work is required to determine how to code these indicators in the image capture. We suggest that future lifelogging privacy research should adopt a model of privacy that incorporates the tension between people's need for interaction and sharing, with their need for privacy or desire to protect the privacy of others[35][6][32] - to account for why people might share images or other data about their friends and other lifeloggers in some contexts, yet delete or keep images private at other times.

Emerging privacy norms within groups should be examined in depth through further field studies by using our toolkit. A particular challenge is how to design the cameras in ways that enable bystanders (known and unknown) to engage in meaningful conversations about their privacy preferences. In the long run, findings of all such studies are likely to facilitate the design and development of intelligent lifelogging cameras, which can detect emerging privacy norms within groups and make recommendations to group members who have not yet customized their privacy settings in line with the group norms.

The issue of bystander awareness of lifeloggers is clearly important; recent work on police use of body cameras [3] suggests that awareness of lifelogging cameras changes the behaviour of the wearer and bystander. We deliberately created a very visible design (bright red, flashing LED) to draw attention to the device but more work is needed to understand how to satisfy both design aesthetics for the wearer and the need to make others aware a camera is present.

Further development of the image reviewing software could also address some of the study limitations and expand our understanding of lifelogging and privacy - for instance, by detecting long timespans between images (where the camera would have been switched off), so participants could have been asked about those times during the end of day review, or doing a 'walk-through' design study where images are reviewed and discussed with the interviewer at the same time, so decisions can be queried and followed up.

While we were able to confirm many of the findings of previous work there were a number of differences. More work is required to unpick these issues and help gather more data to design privacy interfaces that are relevant for both group and single person lifelogging. Our open source hardware and software for conducting visual lifelogging studies should facilitate this future work.

ACKNOWLEDGMENTS

We thank the undergraduate students at the University of Exeter who volunteered their time to wear the cameras and review the many images recorded. The authors acknowledge partial support from EPSRC grants EP/K033433/1, EP/K033522/1 (Privacy Dynamics), EPSRC grant EP/L021285/1 (Monetize Me) as well as the ERC Advanced Grant - Adaptive Security and Privacy (291652 - ASAP), and SFI grant 3/RC/2094.

REFERENCES

[1] Alessandro Acquisti and Ralph Gross. 2006. Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *International workshop on privacy enhancing technologies*. Springer, 36–58. http://link.springer.com/10.1007/11957454_3

[2] Irwin Altman. 1975. *The environment and social behavior : privacy, personal space, territory, crowding.* Brooks/Cole Pub. Co., Monterey, Calif.

[3] Barak Ariel, Alex Sutherland, Darren Henstock, Josh Young, Paul Drover, Jayne Sykes, Simon Megicks, and Ryan Henderson. 2016. "Contagious Accountability" A Global Multisite Randomized Controlled Trial on the Effect of Police Body-Worn Cameras on CitizensâĂŹ Complaints Against the Police. *Criminal Justice and Behavior* (2016), 0093854816668218. http://cjb.sagepub.com/content/early/2016/09/21/0093854816668218.abstract

[4] Richard A Armstrong. 2014. When to use the Bonferroni correction. *Ophthalmic and Physiological Optics* 34, 5 (2014), 502–508.

[5] Lemi Baruh and Zeynep Cemalcilar. 2014. It is more than personal: Development and validation of a multidimensional privacy orientation scale. *Personality and Individual Differences* 70 (Nov. 2014), 165–170. DOI: http://dx.doi.org/10.1016/j.paid.2014.06.042

[6] danah boyd. 2010. Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications. In *Networked Self: Identity, Community, and Culture on Social Network Sites*, Zizi Papacharissi (Ed.). 39–58. http://www.danah.org/papers/2010/SNSasNetworkedPublics

[7] Kelly Erinn Caine. 2009. *Exploring everyday privacy behaviors and misclosures.* PhD. Georgia Institute of Technology. https://smartech.gatech.edu/handle/1853/31665

[8] Jennifer L. Carlson, Mike Paget, and Tim McCollum. 2013. Replicating Two TelePresence Camera Depth-of-Field Settings in One User Experience Study. (2013). http://ceur-ws.org/Vol-976/spaper6.pdf

[9] Soumyadeb Chowdhury, Md Sadek Ferdous, and Joemon M. Jose. 2016. Lifelogging User Study: Bystander Privacy. In *Proceedings of British HCI - Fusion*. BCS, pp. 2.

[10] Soumyadeb Chowdhury, Md Sadek Ferdous, and Joemon M. Jose. 2016. Understanding Lifelog Sharing Preferences of Lifeloggers. In *Proceedings of the 28th Australian Conference on Computer-Human Interaction (OzCHI '16)*. ACM, New York, NY, USA, 649–651. DOI: http://dx.doi.org/10.1145/3010915.3011852

[11] Sarah Clinch, Nigel Davies, Mateusz Mikusz, Paul Metzger, Marc Langheinrich, Albrecht Schmidt, and Geoff Ward. 2016. Collecting Shared Experiences through Lifelogging: Lessons Learned. *Pervasive Computing, IEEE* 15, 1 (2016), 58–67. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=7389256

[12] Alex Fitzpatrick. 2014. Why Google Glass Isn't the Future. *TIME.com* (Nov. 2014). http://time.com/3588143/google-glass/

[13] Ruth Gavison. 1980. Privacy and the Limits of Law. *The Yale Law Journal* 89, 3 (Jan. 1980), 421. DOI: http://dx.doi.org/10.2307/795891

[14] Erving Goffman. 1959. *The Presentation of Self in Everyday Life.* Doubleday, New York.

[15] Cathal Gurrin, Rami Albatal, Hideo Joho, and Kaori Ishii. 2014. A privacy by design approach to lifelogging. *Digital Enlightenment Yearbook* (2014), 49–73.

[16] Andrew F Hayes and Klaus Krippendorff. 2007. Answering the call for a standard reliability measure for coding data. *Communication methods and measures* 1, 1 (2007), 77–89.

[17] S. Hodges, L. Williams, E. Berry, S. Izadi, J. Srinivasan, A. Butler, G. Smyth, N. Kapur, and K. Wood. 2006. SenseCam: A retrospective memory aid. *UbiComp 2006: Ubiquitous Computing* (2006), 177–193.

[18] David Houghton, Adam Joinson, Nigel Caldwell, and Ben Marder. 2013. *Tagger's delight? Disclosure and liking in Facebook: the effects of sharing photographs amongst multiple known social circles.* Technical Report. http://epapers.bham.ac.uk/1723

[19] Roberto Hoyle, Robert Templeman, Denise Anthony, David Crandall, and Apu Kapadia. 2015. Sensitive Lifelogs: A Privacy Analysis of Photos from Wearable Cameras. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM Press, 1645–1648. DOI: http://dx.doi.org/10.1145/2702123.2702183

[20] Roberto Hoyle, Robert Templeman, Steven Armes, Denise Anthony, David Crandall, and Apu Kapadia. 2014. Privacy behaviors of lifeloggers using wearable cameras. *Proceedings of the 16th International Conference on Ubiquitous Computing* (2014), 571–582. DOI: http://dx.doi.org/10.1145/2632048.2632079

[21] Carlos Jensen, Colin Potts, and Christian Jensen. 2005. Privacy Practices of Internet Users: Self-reports Versus Observed Behavior. *Int. J. Hum.-Comput. Stud.* 63, 1-2 (July 2005), 203–227. DOI: http://dx.doi.org/10.1016/j.ijhcs.2005.04.019

[22] Paul Kelly, Simon J. Marshall, Hannah Badland, Jacqueline Kerr, Melody Oliver, Aiden R. Doherty, and Charlie Foster. 2013. An Ethical Framework for Automated, Wearable Cameras in Health Behavior Research. *American Journal of Preventive Medicine* 44, 3 (March 2013), 314–319. DOI: http://dx.doi.org/10.1016/j.amepre.2012.11.006

[23] Marion Koelle, Matthias Kranz, and Andreas MÃűller. 2015. Don't look at me that way!: Understanding User Attitudes Towards Data Glasses Usage. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services*. ACM Press, 362–372. DOI: http://dx.doi.org/10.1145/2785830.2785842

[24] Mohammed Korayem, Robert Templeman, Dennis Chen, David Crandall, and Apu Kapadia. 2014. Screenavoider: Protecting computer screens from ubiquitous cameras. *arXiv preprint arXiv:1412.0008* (2014). http://arxiv.org/abs/1412.0008

[25] David Kushner. 2011. The Making of Arduino. *IEEE Spectrum* (26 Oct. 2011). http://spectrum.ieee.org/geek-life/hands-on/the-making-of-arduino

[26] Carine Lallemand, Vincent Koenig, and Guillaume Gronier. 2013. Replicating an international survey on user experience: challenges, successes and limitations. In *Proceedings of RepliCHI - CHI '13 Extended Abstracts on Human Factors in Computing Systems (CHI EA '13)*. 5.

[27] Clara Mancini, K. Thomas, Y. Rogers, Blaine A. Price, L. Jedrzejczyk, A. K Bandara, A. N Joinson, and B. Nuseibeh. 2009. From spaces to places: emerging contexts in mobile privacy. In *Proc. of UbiComp2009*. 1–10.

[28] Steve Mann. 1998. 'WearCam' (The Wearable Camera): Personal Imaging Systems for long–term use in wearable tetherless computer–mediated reality and personal Photo/Videographic Memory Prosthesis. In *Proceedings of the 2nd IEEE International Symposium on Wearable Computers*. IEEE Computer Society, 124.

[29] Gary T. Marx. 2003. A Tack in the Shoe: Neutralizing and Resisting the New Surveillance. *Journal of Social Issues* 59, 2 (June 2003), 369–390. DOI: http://dx.doi.org/10.1111/1540-4560.00069

[30] Miguel A. Nacenta, Yemliha Kamber, Yizhou Qiang, and Per Ola Kristensson. 2013. Memorability of Pre-designed and User-defined Gesture Sets. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '13)*. ACM, New York, NY, USA, 1099–1108. DOI: http://dx.doi.org/10.1145/2470654.2466142

[31] Narrative. 2017. Narrative Clip. (2017). http://getnarrative.com

[32] Helen Nissenbaum. 2010. *Privacy in Context: Technology, Policy and the Integrity of Social Life*. Standford University Press, Standford, California.

[33] Patricia A. Norberg and Daniel R. Horne. 2007. Privacy attitudes and privacy-related behavior. *Psychology and Marketing* 24, 10 (2007), 829–847. DOI: http://dx.doi.org/10.1002/mar.20186

[34] Open Science Collaboration. 2015. Estimating the reproducibility of psychological science. *Science* 349, 6251 (Aug. 2015), aac4716–aac4716. DOI: http://dx.doi.org/10.1126/science.aac4716

[35] Sandra S. Petronio. 2002. *Boundaries of privacy: dialectics of disclosure*. State University of New York Press.

[36] Rebecca S. Portnoff, Linda N. Lee, Serge Egelman, Pratyush Mishra, Derek Leung, and David Wagner. 2015. Somebody's Watching Me?: Assessing the Effectiveness of Webcam Indicator Lights. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM Press, 1649–1658. DOI: http://dx.doi.org/10.1145/2702123.2702164

[37] S. D. Reicher, R. Spears, and T. Postmes. 1995. A Social Identity Model of Deindividuation Phenomena. *European Review of Social Psychology* 6, 1 (Jan. 1995), 161–198. DOI: http://dx.doi.org/10.1080/14792779443000049

[38] Luis Sanchez, José Antonio Galache, Veronica Gutierrez, Jose Manuel Hernandez, Jesús Bernat, Alex Gluhak, and Tomás Garcia. 2011. Smartsantander: The meeting point between future internet research and experimentation and the smart cities. In *Future Network & Mobile Summit (FutureNetw), 2011*. IEEE, 1–8.

[39] Inc. Snap. 2017. Snapchat Spectacles. (2017). https://www.spectacles.com/

[40] Flávio Souza, Diego de Las Casas, Vinícius Flores, SunBum Youn, Meeyoung Cha, Daniele Quercia, and Virgílio Almeida. 2015. Dawn of the Selfie Era: The Whos, Wheres, and Hows of Selfies on Instagram. In *Proceedings of the 2015 ACM on Conference on Online Social Networks (COSN '15)*. ACM, New York, NY, USA, 221–231. DOI: http://dx.doi.org/10.1145/2817946.2817948

[41] Iuliu Vasilescu, Keith Kotay, Daniela Rus, Matthew Dunbabin, and Peter Corke. 2005. Data collection, storage, and retrieval with an underwater sensor network. In *Proceedings of the 3rd international conference on Embedded networked sensor systems*. ACM, 154–165.

[42] A.F. Westin. 1967. *Privacy and Freedom*. Atheneum. https://books.google.ae/books?id=ydMlnQEACAAJ

[43] Alan F. Westin. 2003. Social and Political Dimensions of Privacy. *Journal of Social Issues* 59, 2 (2003), 431–453. DOI: http://dx.doi.org/10.1111/1540-4560.00072

[44] Max L. Wilson, Ed H. Chi, Stuart Reeves, and David Coyle. 2014. RepliCHI: The Workshop II. In *CHI '14 Extended Abstracts on Human Factors in Computing Systems (CHI EA '14)*. ACM, New York, NY, USA, 33–36. DOI: http://dx.doi.org/10.1145/2559206.2559233

[45] Max L. L. Wilson, Paul Resnick, David Coyle, and Ed H. Chi. 2013. RepliCHI: The Workshop. In *CHI '13 Extended Abstracts on Human Factors in Computing Systems (CHI EA '13)*. ACM, New York, NY, USA, 3159–3162. DOI: http://dx.doi.org/10.1145/2468356.2479636

[46] Mu Yang, Yijun Yu, Arosha K. Bandara, and Bashar Nuseibeh. 2014. Adaptive sharing for online social networks: a trade-off between privacy risk and social benefit. In *Proceedings of 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, 45–52.

Received February 2017; revised April 2017; accepted April 2017